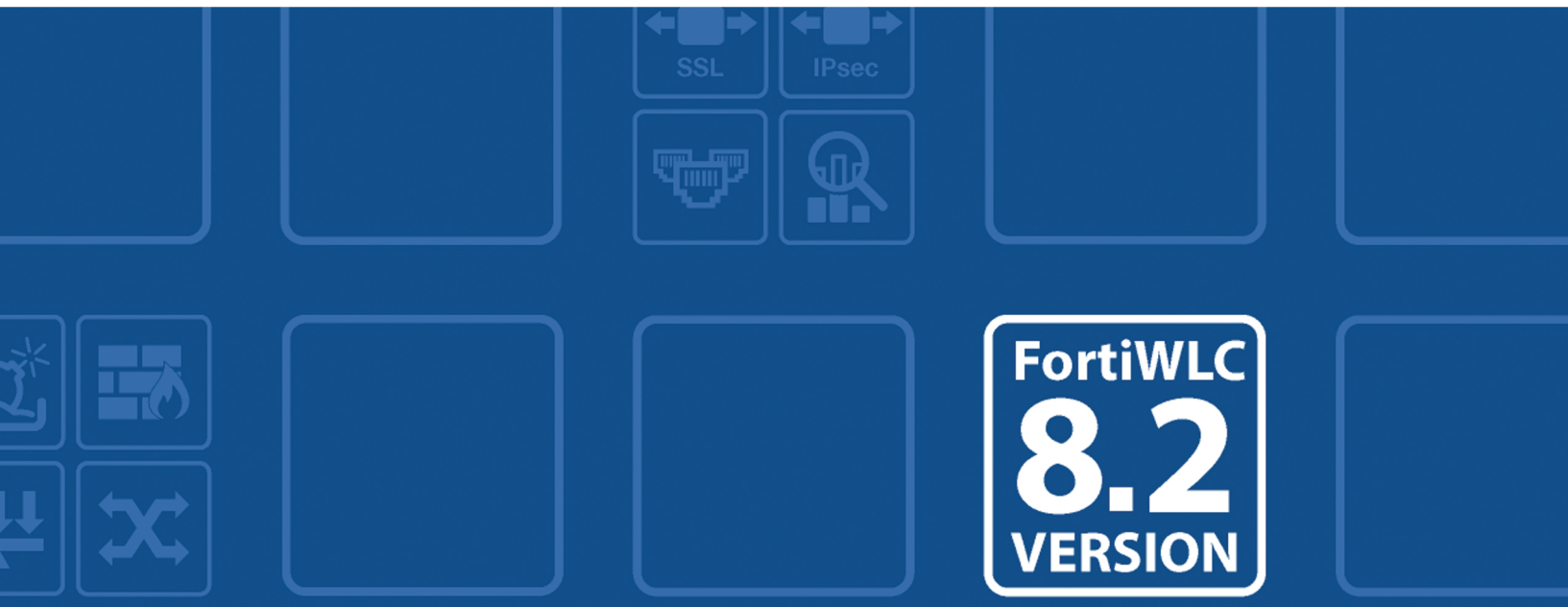
FORTINET®

High Performance Network Security

FortiWLC (SD) - Release Notes

Version 8.2.4



FortiWLC (SD) 8.2 introduces two new 802.11ac Wave2 access points, the FAP U421EV and FAP U423EV. The new Wave2 access points are dual radio, dual band 4x4 four stream 802.11ac Wave 2 access points designed to provide superior experience in data, voice, and video applications in enterprise class deployments.

Fortinet Universal Access Points

FAP-U421EV	FAP-U423EV
	

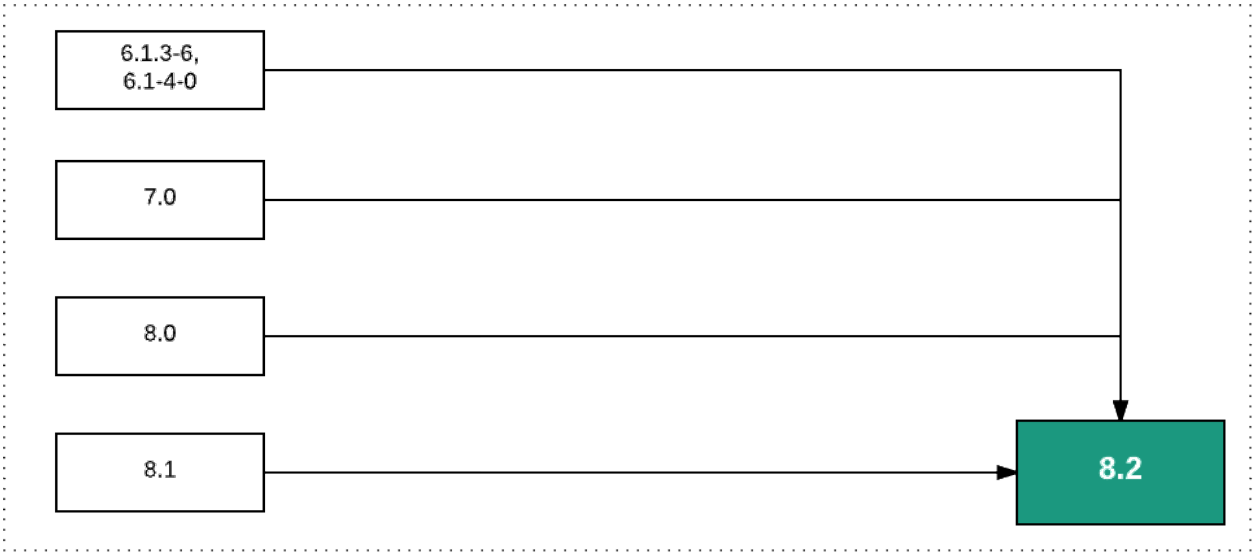
1. FAP-U423EV and FAP-U421EV must be connected only to 802.3at PoE source. Connecting the APs to 802.3af source will not power the radios.
2. When connecting an FAP to a switch, ensure that **portfast** is enabled on the switch port. Refer the switch's configuration guide for more details.

Additionally, this release also introduces features and enhancements as listed under the new features section.

To ensure a secured WiFi network, Fortinet hardware (controllers and access points) are designed to run only the proprietary firmware developed by Fortinet. Only approved Fortinet access points are configurable with Fortinet controllers and vice versa. Third party access points and software cannot be configured on Fortinet hardware.

Getting Started with Upgrade

The following flowchart illustrates the approved upgrade path.



Supported Upgrade Releases

Release	GoTo Release Numbers
6.1	6.1-2-29, 6.1-4
7.0	7.0-1-0, 7.0-2-0, 7.0-3-1, 7.0-4-0. 7.0-9-1,7.0-10-0
8.0	8.0-5-0, 8.0-6-0
8.1	8.1-2-0

Controller upgrade is performed via CLI interface. You will require a serial or SSH2 connection to connect to controller and use its CLI.

Check Available Free Space

Total free space required is the size of the image + 50MB (approximately 230 MB). You can use the **`show file systems`** command to verify the current disk usage.

```
controller# show file systems
Filesystem 1K-blocks Used   Available Use% Mounted on
/dev/hdc2  428972    227844 178242    57%  /
none       4880      56     4824      2%   /dev/shm
none       19528     1788   17740     10%  /opt/meru/var/run
none       9764      240    9524      3%   /opt/meru/var/log
none       9764      68     9696      1%   /tmp
none       9764      0      9764      0%   /opt/meru/capture
```

The first partition (in the above example, /hdc2, although the actual name will vary depending on the version of FortiWLC-SD installed on the controller) is the one that must have ample free space.

In the example above, the partition shows 178242KB of free space (shown bolded above), which translates to approximately 178MB. If your system does not have at least 230MB (230000KB) free, use the **`delete flash:<flash>`** command to free up space by deleting older flash files until there is

enough space to perform the upgrade (on some controllers, this may require deleting the flash file for the current running version).

Set up Serial Connection

Ensure that your serial connection is set for the following options:

Only one terminal session is supported at a time. Making multiple serial connections causes signalling conflicts, resulting in damage or loss of data.

- Baud--115200
- Data--8 bits
- Parity--None
- Stop Bit—1
- Flow Control—None

Supported Hardware and Software

Hardware and Software	Supported		Unsupported
Access Points	AP122 AP822e, AP822i (v1 & v2) AP832e, AP832i, OAP832e AP332e, AP332i* AP433e, AP433i, OAP433e* FAP U421EV FAP U423EV	AP1010e, AP1010i* AP1020e, AP1020i* AP1014i* AP110* AP822 PSM3x*	AP201 AP208 AP150 AP300, AP301, AP302, AP302i, AP301i AP310, AP311, AP320, AP310i, AP320i OAP180 OAP380
*Cannot be configured as a relay AP			
Controllers	FortiWLC 50D FortiWLC 200D FortiWLC 500D MC6000 MC4200 (with or without 10G Module) MC4200-VE MC3200 MC3200-VE MC1550 MC1550-VE		MC 5000 MC 4100 MC 1500 MC 1500-VE
FortiWLM	8.2.2		
FortiConnect	15.10		
Browsers			
FortiWLC (SD) WebUI	Internet Explorer 9,10 Mozilla Firefox 25+ Google Chrome 31+		
A limitation of Firefox 3.0 and 3.5+ prevents display of the X-axis legend of dashboard graphs.			
Captive Portal	Internet Explorer 6, 7, 8, 9, 10, IE11 and Edge. Apple Safari Google Chrome Mozilla Firefox 4.x and earlier Mobile devices (such as Apple iPhone and BlackBerry)		

Upgrading to 8.2-4

1. Open cell is not supported in FAP-U423EV and FAP-U421EV.
2. Virtual cell across Wave1 and Wave2 AP is not supported.

1. Download image files from an FTP or TFTP server to the controller using one of the following commands:

```
# copy ftp://ftpuser:<password@ext-ip-addr>/<?-release-version>-MC_MODEL-rpm.tar<space>.
or
# copy tftp://<ext-ip-addr>/<?-release-version>-MC_MODEL-rpm.tar<space>.
```

? in *<release-version>* is suffixed with meru for MC devices and forti for FWLC devices.

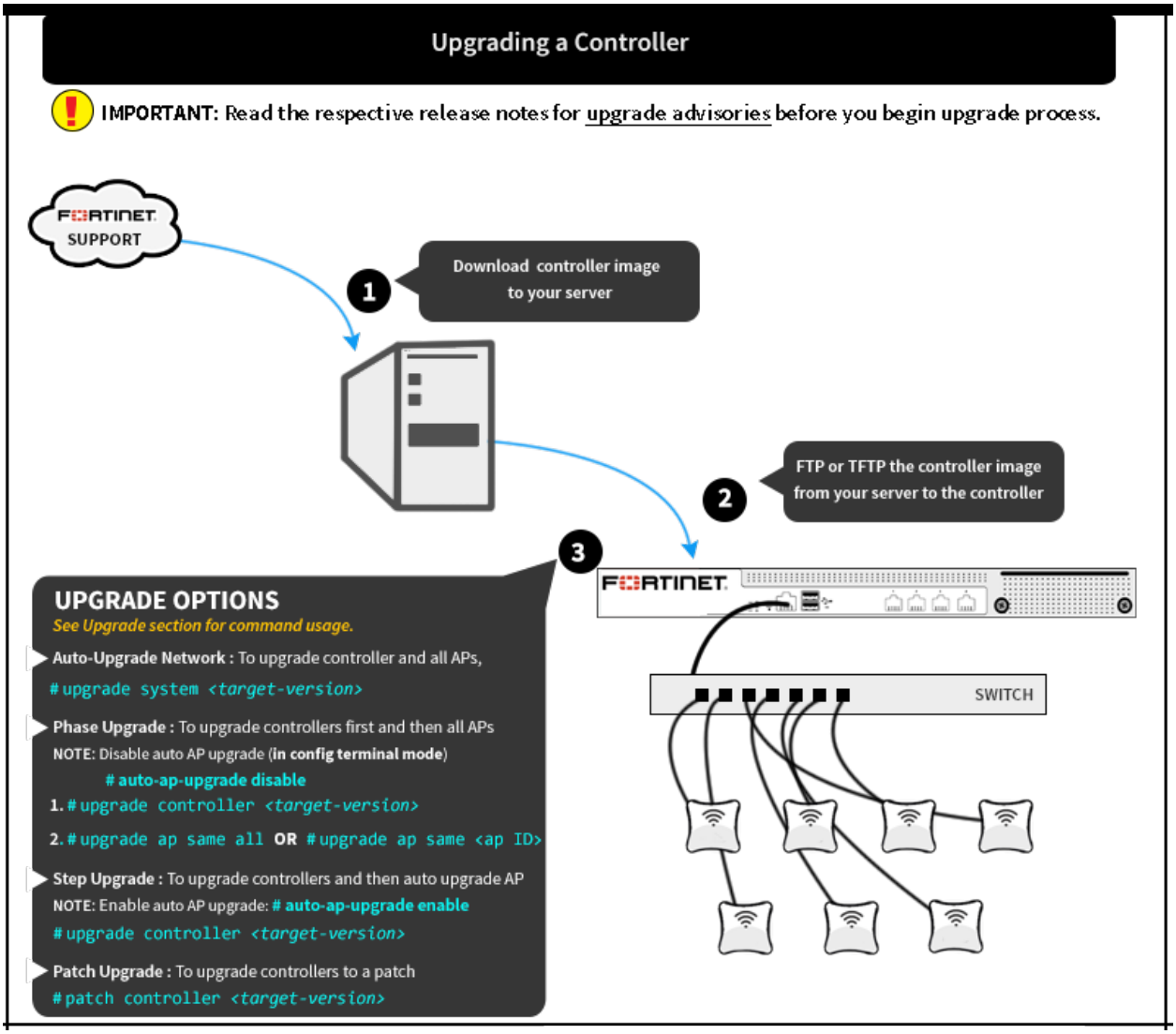
2. Disable AP auto upgrade and then upgrade the controller

```
# configure terminal
# auto-ap-upgrade disable
# copy running-config startup-config
# upgrade controller <target version> (Example, upgrade controller 8.1-2-0)
```

3. Upgrade the APs

```
# upgrade ap same all
```

After the APs are up, use the `show controller` and `show ap` command to ensure that the controller and APs are upgraded to the latest (upgraded) version. Ensure that the system configuration is available in the controller using the `show running-config` command (if not, recover from the remote location). See the Backup Running Configuration step.



Upgrading an N+1 Site

To upgrade a site running N+1, all controllers must be on the same FortiWLC-SD version and the backup controller must be in the same subnet as the primary controllers. You can choose any of the following options to upgrade:

Option 1 - Just like you would upgrade any controller, you can upgrade an N+1 controller.

1. Upgrade master and then upgrade slave.
2. After upgrade, enable master on slave using the `nplus1 enable` command.

Option 2 - Upgrade slave and then upgrade master.

After upgrade, enable master service on slave using the `nplus1 enable` command.

Option 3 - If there are multiple master controllers

1. Upgrade all master controllers followed by slave controllers. After upgrade, enable all master controllers on slave controllers using the `nplus1 enable` command.
2. To enable master controller on slave controller, use the `nplus1 enable` command.

3. Connect to all controllers using SSH or a serial cable.
4. Use the `show nplus1` command to verify if the slave and master controllers are in the cluster. The output should display the following information:

```
Admin: Enable
Switch: Yes
Reason: -
SW Version: 8.2-3
```

5. If the configuration does not display the above settings, use the `nplus1 enable <master-controller-ip>` command to complete the configuration.
6. To add any missing master controller to the cluster, use the `nplus1 add master` command.

Restore Saved Configuration

1. Copy the backup configuration back to the controller:

```
# copy ftp://<user>:<passswd>@<offbox-ip-address>/runningconfig.txt orig-config.txt
```

2. Copy the saved configuration file to the running configuration file:

```
# copy orig-config.txt running-config
```

3. Save the running configuration to the start-up configuration:

```
# copy running-config startup-config
```

Upgrade Advisories

The following are upgrade advisories to consider before you begin upgrading your network.

Devices with Intel Chipset 62xx

Wireless devices with Intel chipset 62xx series must upgrade its firmware to version 18.20.x.x.

Mesh Deployments

When attempting to upgrade a mesh deployment, you must start upgrading the mesh APs individually, starting with the outermost APs and working inwards towards the gateway APs before upgrading the controller. *Be sure to disable the auto-ap-upgrade feature when performing this task*. The following procedure is recommended for optimal operation:

1. Disable the **`auto-ap-upgrade`** feature.
2. Copy the running-config to startup-config.
3. Upgrade the APs manually using `upgrade ap same all` command.

In order to prevent IP assignment problems after the upgrade, if your network utilizes VLAN configurations, ensure that the DHCP Relay Pass-through option is enabled in the following two locations:

- **Configuration** > **Devices**: *Controller*
- **Configuration** > **Wired**: *VLAN* > [Select VLAN]

Captive Portal and Fortinet Connect Deployment Recommendations

DNS Entry

It is mandatory to enter the DNS while creating internal DHCP profile.

External Portal IP Configuration:

If a NAT device is located between the controller and the Fortinet Connect, the IP address with which Fortinet Connect sees the controller should be configured under Device > RADIUS Clients page in Fortinet Connect Admin portal (*http://<fortinetconnect-ip-address>/admin*), . Select the RADIUS client and enter the controller IP address in the Client tab. The Fortinet Connect Automatic Setup then configures the controller correctly and ensures that the correct controller IP address is configured on Fortinet Connect.

Remember Me settings

In the Portal Settings step of the Guest Portal configuration wizard, if you choose to enable Remember Credentials, then select "Initially attempt to use a cookie, if that fails try the MAC address" option. This removes dependency on the client's browser and security settings.

SmartConnect Certificate download

In the Certificates step of the Smart Connect Profile Wizard, ensure that you select the complete certificate chain of your uploaded certificate. If you have uploaded all certificates in the chain (from root to server), then selecting the server certificate will automatically select the entire certificate chain.

- To upload the server certificates, goto **Server** > **SSL Settings** > **Server Certificate** tab.
- To upload rest of the chain, goto **Server** > **SSL Settings** > **Trusted CA Certificates** tab.

Chromecast Discovery

To ensure a Chromecast device receives packet from a client (publisher), both, the Chromecast device and the client must be in the same subnet. This is applicable to Chromecast version 1 and version 2.

CNA Bypass for Android 5.0 +

Devices running Android 5.0 and above introduces system default CP login pop-up windows. To disable this pop-up window enable CNA bypass in the controller.

In the WebUI

Go to **Configuration** > **Security** > **Captive Portal** > Advanced Settings section, select Captive Portal Prole and set **Apple Captive Network Assistant (CNA) Bypass** to **ON**.

Using CLI

Use the **`ssl-server cna-bypass ON`** command in config mode.

Voice Scale Recommendations

The following voice scale settings are recommended if your deployment requires more than 3 concurrent calls to be handled per AP. The voice scale settings are enabled for an operating channel (per radio). When enabled, all APs or SSIDs operating in that channel enhances voice call service. To enable:

1. In the WebUI, go to **Configuration** > **Devices** > **System Settings** > **Scale Settings** tab.
2. Enter a channel number in the *Voice Scale Channel List* field and click **OK**.

Enable the voice scale settings only if the channel is meant for voice deployment. After enabling voice scale, the voice calls in that channel take priority over data traffic and these results in a noticeable reduction of throughput in data traffic.

IP Prefix Validation

In a situation where a station with an IP address from a different subnet connects to the controller, it can result in various network issues including outage. A new field, IP Prefix Validation is added to the ***ESS Profile*** and ***Port Profile*** configuration page. When enabled, stations with different subnet are prevented from connecting to the controller. By default, IP Prefix Validation in **ESS Profile is ON** and in **Port Profile it is OFF**.

QoS Rules

QoS rules with no matching criteria when *Match* is checked will abort an upgrade. To prevent this, check QoS rules to ensure that at least one matching criteria is set for each rule if *Match* is set.

Downgrade Procedure

Any controller that has been upgraded to 8.2-4 can only be downgraded to the previous release from which it was originally upgraded.

Obtain a signed image file for a downgrade from the FTP site and install it on the controller before the downgrading. To downgrade to an earlier release, use the upgrade procedure. Before downgrading to any release, save your configuration to a backup file and store it on a server accessible by FTP. The saved configuration can then be used to restore your configured parameters if needed. There are two upgrade command options.

You can upgrade the controller first using the **`upgrade controller`** command and then upgrade APs using the **`upgrade ap same all`** command. You can also use the **`upgrade system`** command; this downgrades the APs first, then the controller.

New Features

- Social Authentication Support in Captive Portal
- Support for WPA2-TKIP encryption
- Logical Grouping of ESS and Security Config Options
- MU-MIMO Configuration
- PoE Redundancy

Social Authentication Support in Captive Portal

The captive portal authentication process now supports Fortinet Presence as an external CP authentication server that allows users to authentication using social media accounts like Facebook or Gmail OAuth.

Supported APs: AP122, AP822, AP832, OAP832, FAP-U421, and FAP-U423

Before proceeding, note the following:

- Enable location service in the controller (See *Configuring FortiPresence API* section in the FortiWLC (SD) configuration guide for more details).
- Assign the AP in the data analytics store.
- Not supported in "Bridge mode".

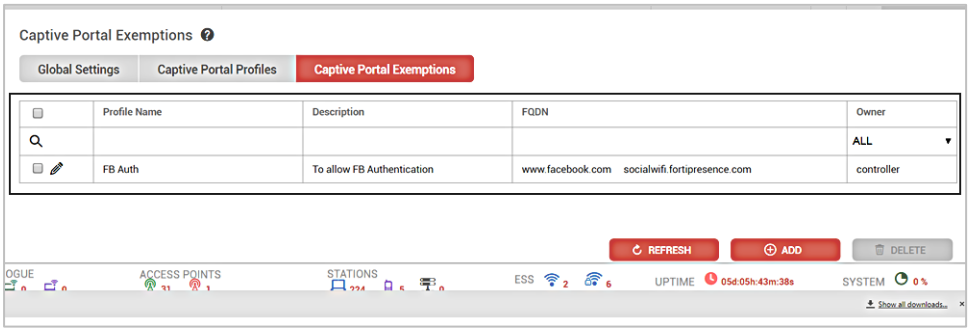
To enable social authentication support, do the following:

1. Create captive portal exemptions profile
2. Configure captive portal profile to use Fortinet Presence
3. Enable this captive portal profile in security profile and add this security profile in the ESS profile.

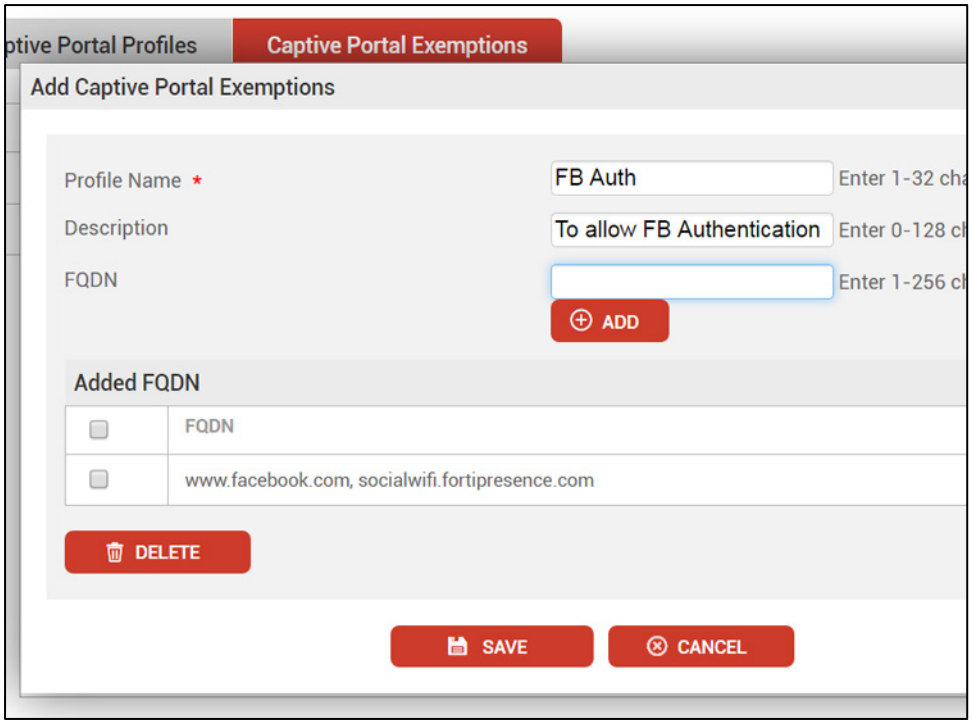
Create Captive Portal Exemptions Profile

To enable social login, create a profile with the list of exempted URLs and in the captive portal profile and select FortiPresence as the external authentication server.

1. Go to Configuration > Security > Captive Portal > Captive Portal Exemptions.



2. Click the **Add** button to create a profile with the list of URLs that will be allowed for social authentications. To add multiple URL to a profile, enter a space after each URL entry. You can add up to 32 URLs.

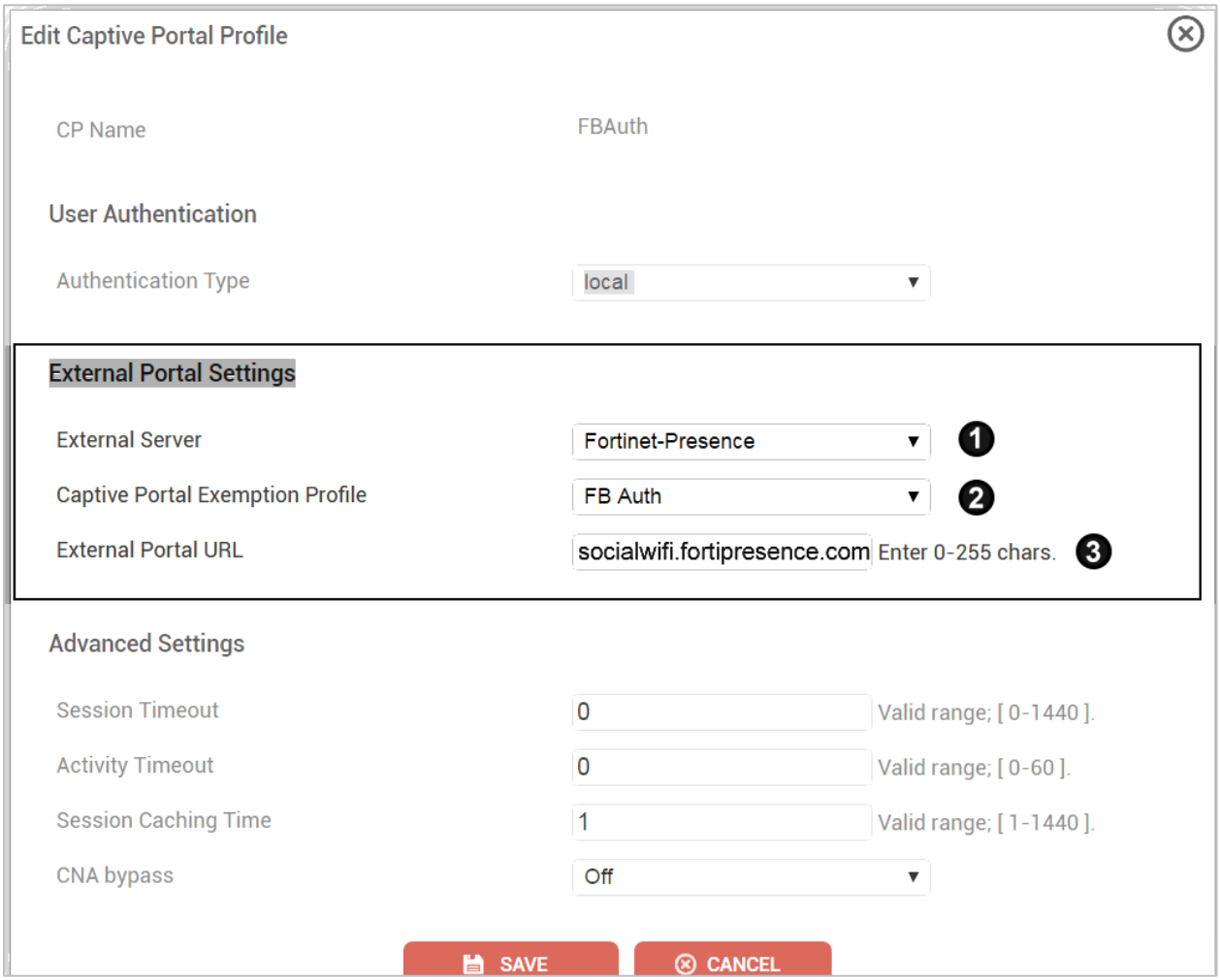


For each profile, ensure that you add **socialwifi.fortipresence.com** (inclusive of the 32 URLs) as part of the FQDN list. This is mandatory for clients to access Social Wi-Fi login page.

Configure Captive Portal Profile to use Fortinet Presence

1. Go to Configuration > Security > Captive Portal > Captive Portal Profiles page
2. Create a captive portal profile with ***local*** or ***radius*** as authentication type.
    a. If Authentication type is ***Local***, then create a guest user with the following credentials:
        - username: `gooduser`
        - password: `good`
    b. If Authentication type is ***RADIUS***, then in that RADIUS server, create a user with the following credentials:
        - username: `gooduser`
        - password: `good`

3. Make the following changes to External Portal Settings:



1. Select Fortinet-Presence as the external server (1).
2. Select the profile (2) created with the exempted URLs.
3. Enter **http://socialwifi.fortipresence.com/wifi.html?login** as URL (3) in the external portal URL.

For Fortinet Presence server configuration and account, see the FortiPresence configuration guide: http://docs.fortinet.com/d/fortipresence-analytics-configuration-guide

Enable this captive portal profile in security and ESS profiles

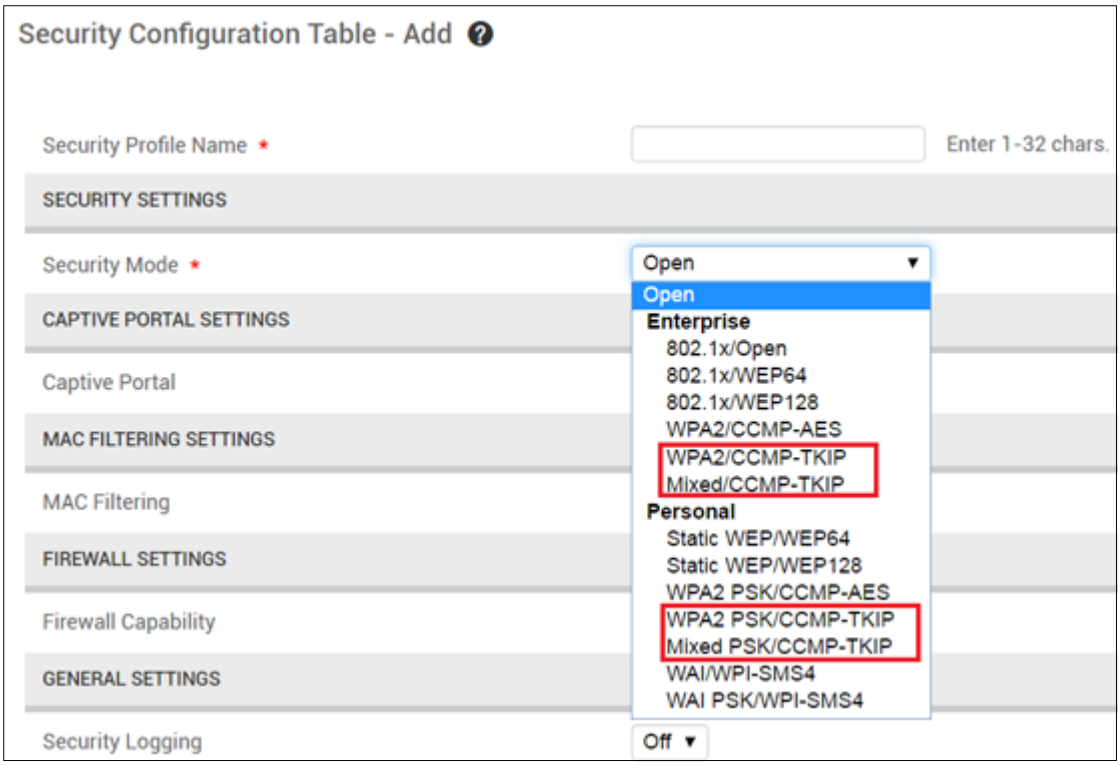
Enable the captive portal profile in the security profile and map the security profile in the ESS Profile. In the security profile, make the following changes to the CAPTIVE PORTAL SETTINGS section:

1. Set Captive Portal to ***Webauth***.
2. Select the captive portal created for enabling social Wi-Fi login.
3. Set Captive Portal Authentication Method as External.

In the ESS-Profile set Dataplane mode to **Tunnel Mode**.

Support for WPA2-TKIP encryption

You can now create a security profile with WPA2-TKIP encryption. This option is available in the security mode dropdown list in the security profile configuration page (**Configuration** > **Security** > **Profile** (*Add and Edit pages*)):

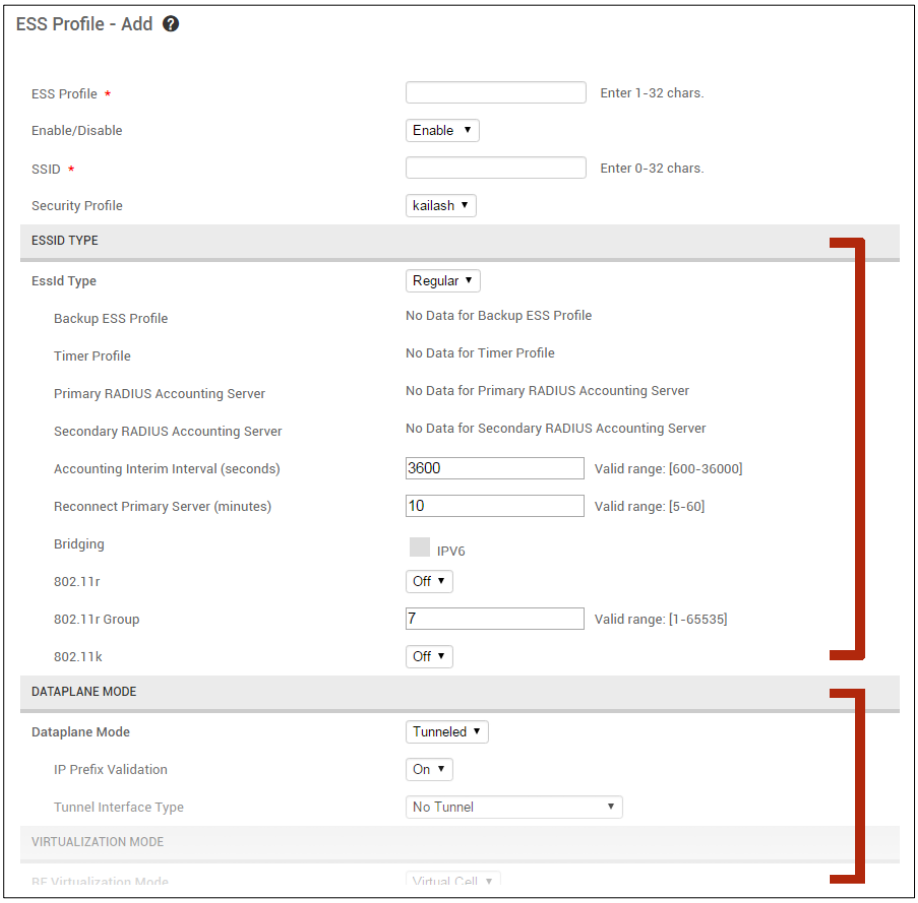


It is important to note that TKIP encryption is less secure than AES and is not a recommended encryption method.

Logical Grouping of ESS and Security Config Options

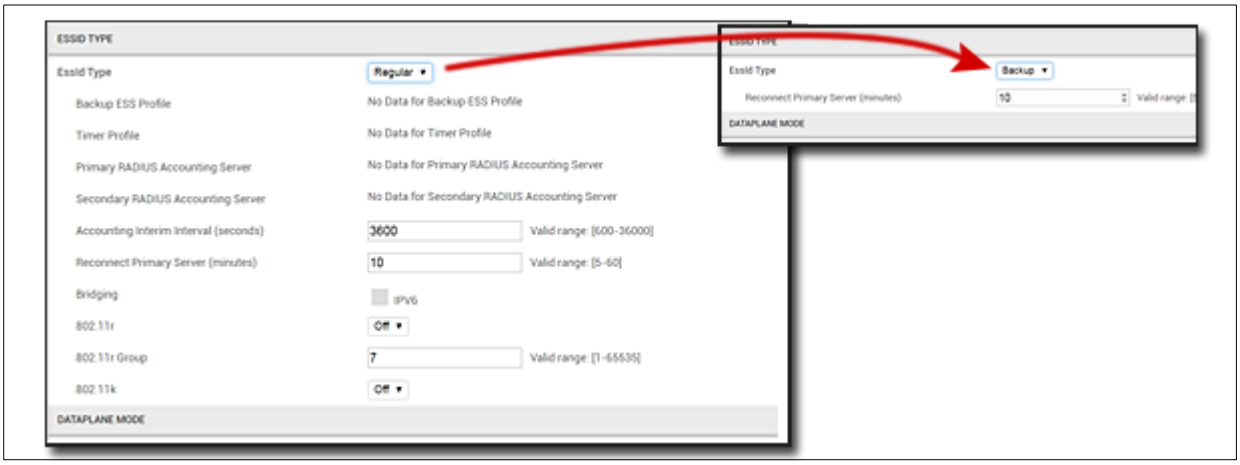
Starting with release 8.2, ESS and Security profile config options in the WebUI are grouped logically to help in easy configuration.

ESS Profile



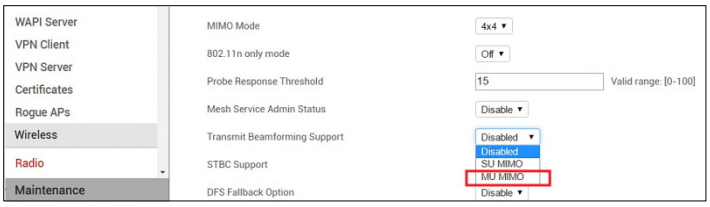
Security Profile

Additionally, within the logical groups' only dependent configuration options of a parameter are visible. For example, in an ESS profile selecting the Essid Type as *Backup*, shows parameters that are applicable only for a backup ESS profile.



MU-MIMO Configuration

A new configuration parameter MU-MIMO is added to the radio configuration that allows multiple Tx beamforming. If your network has MU-MIMO capable clients (802.11ac Wave 2), then we recommend enabling this parameter. By default, this option is enabled.



1. MU- MIMO is supported only on a single ESS profile
2. Supports one group with a maximum of 3 clients. If additional MU-MIMO clients join the network, groups are not created dynamically.
3. 2x2 and 3x3 clients are not supported in MU-MIMO mode.
4. 160MHz is not supported.

PoE Redundancy

The FAP U421EV and U423EV access point's physical interfaces LAN1 and LAN2 can be used for powering on and to provide regular WLAN functionalities.

Fixed Issues

Bug ID	Description	Scenario
0381099	Fixed issues that caused incorrect AP model name to be displayed in the “show alarm” command output.	The issue was found in release 8.2.
380543	Fixed issues that resulted in missing information regarding Ethernet statistics via GUI and CLI.	The issue was noticed in 8.2-1-0.
380539	Fixed incorrect information regarding AP PoE connection.	There was an issue that resulted in the GUI page (Configuration > APs > <ap-ID) > >Ethernet Interface) displayed incorrect information about APs LAN port.
379218	Fixed incorrect data reporting on the radio dashboard.	The issue was noticed in release 8.2-1-0.
379217	Enabled options to turn off LED lights.	NA
373406	AP tables in WebUI will have a MAC address column instead of the serial number column.	There was an issue where the column header was labelled as Serial Number but the column displayed MAC address. This issue was seen in 8.1 and is now fixed.
0384697	Fixed issues that prevented adding a master to slave.	This issue was noticed after upgrading from 8.1 to 8.2 without N+1 configuration.

Known Issues

Bug ID	Description
376269	In a non-link aggregation scenario, FAPs 421/423 will reboot if one of the link goes down.
375673	TX stuck leading to Beacon misses and causing client connectivity issues. **Workaround**: Use ESS profile in tunnelled mode for multicast traffic.
0381841	Performance degradation is observed when UAPSD is on for FAP421/423 APs.
0377688	Observed low throughput with lots of wl1: PHYTX error message for 4x4 11ac clients.
0383546	FAP is unable to discover the controller when a PoE switch is connected to the LAN2 port Profile. **Workaround**: This happens when port profile is used to extend network. In such scenario, use LAN2 for uplink.
0375671	Ack is not returned for QOS Null frames.
0382011, 0381334	Performance degradation is observed in a mixed client (MU-MIMO and SU-MIMO) environment.

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

Contact

For assistance, contact Fortinet Customer Service and Support 24 hours a day at +1 408-542-7780, or by using one of the local contact numbers, or through the Support portal at https://support.fortinet.com/

Fortinet Customer Service and Support provide end users and channel partners with the following:

- Technical Support
- Software Updates
- Parts replacement service